



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/702,540	11/07/2003	Vincent So	79865-5 /aba	8250

7380 7590 12/07/2007
SMART & BIGGAR
P.O. BOX 2999, STATION D
900-55 METCALFE STREET
OTTAWA, ON K1P5Y6
CANADA

EXAMINER

AGWUMEZIE, CHARLES C

ART UNIT	PAPER NUMBER
----------	--------------

3621

MAIL DATE	DELIVERY MODE
-----------	---------------

12/07/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/702,540	Applicant(s) SO, VINCENT	
	Examiner Charlie C. Agwumezie	Art Unit 3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 20 September 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-23 and 34-43 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-23 and 34-43 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>11/7/03 & 9/28/07</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Acknowledgements

1. In view of the appeal brief filed on September 20, 2007, **PROSECUTION IS HEREBY REOPENED**. An office action is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

- (1) file a reply under 37 CFR § 1.111 (if this Office action is non-final); or,
- (2) request reinstatement of the appeal. If reinstatement of the appeal is requested, such request must be accompanied by a supplemental appeal brief, but no new amendments, affidavits (37 CFR § 1.130, 1.131, or 1.132) or other evidence are permitted. See 37 CFR 1.193(b)(2).

Claims status

2. Claims 1-23 and 34-43 remain pending in this application.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1, 7-10, 13, 15, 35-38, and 40-42, are rejected under 35 U.S.C. 103(a) as being unpatentable over Peterka et al U.S. Patent Application Publication No. 2002/0170053 A1 in view of Feig et al U.S. patent No. 7,251,833 B2.

As per **claims 1, 15 and 38**, Peterka et al discloses a method of delivering data content from a data content provider to a customer processing platform and controlling use of the data content at the customer processing platform, comprising:

encrypting each of a plurality of sections of the data content using a respective one of a plurality of encryption keys to produce a corresponding plurality of encrypted sections (0080, which discloses that "a caching server may divide the content into pay segments and assign segment keys to them"; 0082; 0101);

delivering the plurality of encrypted sections to the customer processing platform (fig. 8; 0080, which discloses "dividing the content into pay segments"; 0082, which discloses that "start receiving multicast content").

What Peterka et al does not explicitly disclose is

delivering to the customer processing platform a plurality of decryption keys corresponding to the plurality of encryption keys, wherein the decryption keys are delivered in a manner such that the customer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time. Peterka however discloses discloses that "two PSK are distributed at a given time"; that a client has possession of program segment key and the next key...as well as content key 0, 1, 2, 3, 4,

Feig et al discloses a method of delivering data content from a data content provider to a customer processing platform and controlling use of the data content at the customer processing platform, comprising:

delivering to the customer processing platform a plurality of decryption keys corresponding to the plurality of encryption keys, wherein the decryption keys are delivered in a manner such that the customer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time (see fig. 3, step 308-314; col. 2, lines 40-65, which discloses that "it is preferred that the token keys are transmitted to the client receiver by sequentially streaming each of the token keys, one at a time, enabling a one-to-one decryption and playback of the encrypted sequential data blocks"; col. 3, lines 1-5, which discloses that preferred method further includes sequentially decrypting each of the respective plurality of encrypted sequential data blocks using corresponding one of the plurality of cryptographic token keys...and for playing back each recovered sequential data").

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Peterka et al and incorporate the method wherein the decryption keys are delivered in a manner such that the customer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time in view of the teachings of Feig et al in order to ensure that content is only used by authorized users since usage is under the control of the server.

As per **claim 7**, Peterka et al further discloses the method further comprising:

billing a customer for delivery of the encrypted sections, and then billing the customer each time the data content is used at the customer processing platform (figs. 8 and 9; 0111, "billing system to analyze ...determine the length of content watched by each client").

As per **claim 8**, Peterka et al further discloses the method, wherein the data content is video content or music content, and wherein use of the data content at the customer processing platform comprises decryption and playback of the data content (0048, "music event"; 0080; 0082).

As per **claim 9**, Peterka et al further discloses the method, wherein each of the plurality of encryption keys comprises a respective symmetric cryptographic key, and wherein each of the plurality of decryption keys comprises the symmetric cryptographic key of its corresponding encryption key (0006, "cryptographic keys"; 0080; 0082; 0117).

As per **claim 10**, Peterka et al further discloses the method, further comprising:
generating each of the plurality of encryption keys using an identifier associated with the customer processing platform, to thereby generate a plurality of customer processing platform-specific keys (see fig. 21; 0146, "receives a program content identifier from client"; 0114; 0124).

As per **claim 13**, Peterka et al further discloses the method, further comprising:

generating a respective transmission value for each of the plurality of encryption keys using an identifier associated with the customer processing platform (0097; 0114; 0124; claim 23),

wherein delivering to the customer processing platform a plurality of decryption keys comprises delivering the transmission values (0097; 0114; 0124; claim 23).

As per claims 35, and 37, Peterka et al discloses a computer readable medium storing software code executable by a processing platform, the software code comprising:

first software code for coordinating downloading a plurality of sections of data content each encrypted with a respective one of a plurality of encryption keys to a customer computer system from a data content service provider system or another customer computer system (fig. 7; 0080; 0082; 0101).

What Peterka et al does not explicitly disclose is

second software code for establishing a connection with the data content service provider system to obtain permission to use the data content, and for using the data content where permission is obtained from the data content service provider system by receiving a corresponding one of a plurality of decryption keys for each encrypted section of data content and decrypting the encrypted section using the corresponding one of the plurality of decrypting keys such that the processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time.

Feig et al discloses a second software code for establishing a connection with the data content service provider system to obtain permission to use the data content, and for using the data content where permission is obtained from the data content service provider system by receiving a corresponding one of a plurality of decryption keys for each encrypted section of data content and decrypting the encrypted section using the corresponding one of the plurality of decrypting keys such that the processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time (see fig. 3, step 308-314; col. 2, lines 40-65, which discloses that "it is preferred that the token keys are transmitted to the client receiver by sequentially streaming each of the token keys, one at a time, enabling a one –to-one decryption and playback of the encrypted sequential data blocks"; col. 3, lines 1-5, which discloses that preferred method further includes sequentially decrypting each of the respective plurality of encrypted sequential data blocks using corresponding one of the plurality of cryptographic token keys...and for playing back each recovered sequential data").

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Peterka et al and incorporate the method wherein second software code for establishing a connection with the data content service provider system to obtain permission to use the data content, and for using the data content where permission is obtained from the data content service provider system by receiving a corresponding one of a plurality of decryption keys for each encrypted section of data content and decrypting the encrypted section using the corresponding one of the plurality of decrypting keys such that the processing platform

has simultaneous possession of at most a subset of the plurality of decryption keys at any time in view of the teachings of Feig et al in order to ensure that content is only used by authorized users since usage is under the control of the server.

As per **claim 36**, Peterka et al further discloses the computer readable medium, wherein the second software code obtains further permissions from the data content service provider system to continue using the data content (see fig. 15; ...permit the client who received the second key to decrypt the encrypted program content...; 0094, "continue viewing the remainder of the content...").

As per **claim 40**, Peterka et al discloses a data content distribution system comprising:

a data content server configured to receive download requests and permission requests for data content, to encrypt a plurality of sections of requested data content using respective encryption keys to thereby generate a plurality of encrypted sections and to transmit the encrypted sections of the data content in response to a received download request for the data content, and to transmit each of a plurality of decryption keys respectively corresponding to the encryption keys in response to a permission request for the data content (figs. 1, 3, 8, 9 and 15).

What Peterka does not explicitly disclose is:

a data content download controller configured to generate download requests, to receive encrypted sections of data content in response to download requests, to

generate permission requests when downloaded data content is to be used, and for each encrypted section of data content to be used, to receive a corresponding one of the plurality of decryption keys, and to decrypt the encrypted section using the corresponding one of the plurality of decryption keys, said data content server to transmit the plurality of decryption keys in a manner such that the data content download controller has simultaneous possession of at most a subset of the plurality of decryption keys at any time.

Feig et al discloses a data content download controller configured to generate download requests, to receive encrypted sections of data content in response to download requests, to generate permission requests when downloaded data content is to be used, and for each encrypted section of data content to be used, to receive a corresponding one of the plurality of decryption keys, and to decrypt the encrypted section using the corresponding one of the plurality of decryption keys, said data content server to transmit the plurality of decryption keys in a manner such that the data content download controller has simultaneous possession of at most a subset of the plurality of decryption keys at any time (see fig. 3, step 308-314; col. 2, lines 40-65, which discloses that "it is preferred that the token keys are transmitted to the client receiver by sequentially streaming each of the token keys, one at a time, enabling a one-to-one decryption and playback of the encrypted sequential data blocks"; col. 3, lines 1-5, which discloses that preferred method further includes sequentially decrypting each of the respective plurality of encrypted sequential data blocks using corresponding one

of the plurality of cryptographic token keys...and for playing back each recovered sequential data").

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Peterka et al and incorporate the method wherein a data content download controller configured to generate download requests, to receive encrypted sections of data content in response to download requests, to generate permission requests when downloaded data content is to be used, and for each encrypted section of data content to be used, to receive a corresponding one of the plurality of decryption keys, and to decrypt the encrypted section using the corresponding one of the plurality of decryption keys, said data content server to transmit the plurality of decryption keys in a manner such that the data content download controller has simultaneous possession of at most a subset of the plurality of decryption keys at any time in view of the teachings of Feig et al in order to ensure that content is only used by authorized users since usage is under the control of the server.

As per claim 41, Peterka et al further discloses the system, comprising a data network connecting the data content server and the data content download controller (fig. 1).

As per claim 42, Peterka et al further discloses the system, further comprising a plurality of data content download controllers connected to the data network (fig. 1).

4. Claims 2-6, 34, and 39, are rejected under 35 U.S.C. 103(a) as being unpatentable over Peterka et al U.S. Patent Application Publication No. 2002/0170053 A1 in view of Feig et al U.S. patent No. 7,251,833 B2 and further in view of Giroux et al U.S. Patent No. 2002/0078361 A1.

As per claim 2, Peterka et al further discloses the method, wherein delivering to the customer processing platform a plurality of decryption keys comprises:

delivering to the customer processing platform a first key of the plurality of decryption keys for a first encrypted section of the plurality of encrypted sections (figs. 3 and 6; 0007, "request first key"; 0080 "assign segment keys; 0102, "current PSK");

delivering to the customer processing platform a second key of the plurality of decryption keys for a second encrypted section of the plurality of encrypted sections (0007, "distribute second key"; 0102, "next key").

What Peterka et al does not explicitly teach is

causing the first key to be destroyed at the customer processing platform.

Giroux et al discloses the method of delivering data content comprising causing the first key to be destroyed at the customer processing platform (0051, which discloses that "after decrypting the section, ... immediately discards/destroys the key...").

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Peterka et al and incorporate the method of delivering data content comprising causing the first key to be destroyed at the

customer processing platform in view of the teachings of Giroux et al in order to ensure that content is only used for the number of times permitted.

As per claim 3, Peterka et al further discloses the method, wherein delivering to the customer processing platform a plurality of decryption keys comprises:

delivering to the customer processing platform a current key of the plurality of decryption keys for a current encrypted section of the plurality of encrypted sections to be processed at the customer processing platform (0007, "request first key"; 0080 "assign segment keys; 0102, "current PSK");

delivering to the customer processing platform a next key of the plurality of decryption keys for a next encrypted section of the plurality of encrypted sections to be subsequently processed at the customer processing platform upon completion of processing of the current encrypted section (0080; 0082; 0102; ...client has possession of program segment key and next key..."; 0102, "next key").

What Peterka et al does not explicitly teach is

causing the first key to be destroyed at the customer processing platform.

Giroux et al discloses method of delivering data content comprising causing the first key to be destroyed at the customer processing platform (0051, which discloses that "after decrypting the section, ... immediately discards/destroys the key...").

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Peterka et al and incorporate the method of delivering data content comprising causing the first key to be destroyed at the

customer processing platform in view of the teachings of Giroux et al in order to ensure that content is only used for the number of times permitted.

As per **claim 4**, Peterka et al further discloses the method, wherein delivering to the customer processing platform a next key of the plurality of decryption keys (0080; 0082) and

What Peterka does not explicitly teach is causing the current key to be destroyed at the customer processing platform are repeated for each of the plurality of encrypted sections to be subsequently processed.

Giroux et al discloses causing the current key to be destroyed at the customer processing platform are repeated for each of the plurality of encrypted sections to be subsequently processed (0051, which discloses that "after decrypting the section ... immediately discards/destroys the key ... when the viewing user moves to a different section, the process is repeated").

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Peterka et al and incorporate the method of causing the current key to be destroyed at the customer processing platform are repeated for each of the plurality of encrypted sections to be subsequently processed in view of the teachings of Giroux et al in order to ensure that content is only used for the number of times permitted.

As per **claim 5**, Peterka et al discloses the method, wherein the current

encrypted section is a first one of the plurality of encrypted sections (0080; 0082), and wherein delivering to the customer processing platform a next key of the plurality of decryption keys (0080; 0082).

What Peterka et al does not explicitly teach is causing the current key to be destroyed at the customer processing platform are repeated for each of the plurality of encrypted sections following the first encrypted section.

Giroux et al discloses causing the current key to be destroyed at the customer processing platform are repeated for each of the plurality of encrypted sections following the first encrypted section (0051, which discloses that "after decrypting the section ... immediately discards/destroys the key ... the clears the buffers to destroy the decrypted versions of the section").

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Peterka et al and incorporate the method of delivering data content comprising causing the current key to be destroyed at the customer processing platform are repeated for each of the plurality of encrypted sections following the first encrypted section in view of the teachings of Giroux et al in order to ensure that content is only used for the number of times permitted.

As per **claim 6**, Peterka et al further discloses the method, wherein delivering to the customer processing platform a plurality of decryption keys comprises:

providing key control software to the customer processing platform, the key control software being adapted to: receive a decryption key for one of the plurality of encrypted sections (0080; 0082; 0117; 0118);

complete decryption of the one section (0080; 0082).

What Peterka et al does not explicitly teach is

destroy the decryption key.

Giroux et al discloses a method comprising destroy the decryption key (0051, which discloses that "after decrypting the section ... immediately discards/destroys the key...").

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Peterka et al and incorporate the method of destroy the decryption key in view of the teachings of Giroux et al in order to ensure that content is only used for the number of times permitted.

As per claim 34, Peterka et al further discloses a method for controlling use of encrypted data content downloaded to a customer data content processing device, comprising:

receiving a request comprising customer verification information from a customer data content processing device (0072; 0123; 0145);

comparing the customer verification information with corresponding stored customer information (0145); and

where the customer verification information is consistent with the stored customer verification information:

billing a usage charge to an account of the customer (figs. 8 and 9);

transmitting to the customer data content processing device a digital key to decrypt a current portion of the encrypted data content (fig. 5; 0145); and

for each subsequent portion of the encrypted data:

transmitting to the customer data content processing device a different key to decrypt the subsequent portion of the encrypted data.

What Peterka et al does not explicitly teach is

for each subsequent portion of the encrypted data:

transmitting to the customer data content processing device a different key to decrypt the subsequent portion of the encrypted data.

causing a key for a preceding portion of the encrypted data to be deleted from the customer data content processing device.

Feig et al discloses:

for each subsequent portion of the encrypted data:

transmitting to the customer data content processing device a different key to decrypt the subsequent portion of the encrypted data (col. 2, lines 40-65, "one to one decryption").

Giroux et al discloses a method of causing a key for a preceding portion of the encrypted data to be deleted from the customer data content processing device (0051,

Art Unit: 3621

which discloses that "after decrypting the section, ... immediately discards/destroys the key...").

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Peterka et al and incorporate the method of causing a key for a preceding portion of the encrypted data to be deleted from the customer data content processing device in view of the teachings of Giroux et al in order to ensure that content is only used for the number of times permitted.

As per claim 39, Peterka et al further discloses the system, wherein the customer processing platform comprises:

means for requesting the data content to be delivered to the customer processing platform (fig. 1);

means for receiving the plurality of encrypted sections (0080; 0082);

means for receiving, for each encrypted section, the decryption key in respect of the encrypted section (0080; 0082);

means for decrypting and playing back the encrypted section using the decryption key (0080; 0082).

What Peterka et al does not explicitly teach is

means for destroying the decryption key, after completing playback of the encrypted section.

Giroux et al discloses means for destroying the decryption key, after completing playback of the encrypted section (0051, which discloses that "after decrypting the section, ... immediately discards/destroys the key...").

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Peterka et al and incorporate the method of destroying decrypted data content at the customer processing platform after completing playback of the encrypted section in view of the teachings of Giroux et al in order to ensure that content is only used for the number of times permitted.

5. **Claims 11, and 12**, are rejected under 35 U.S.C. 103(a) as being unpatentable over Peterka et al U.S. Patent Application Publication No. 2002/0170053 A1 in view of Feig et al U.S. patent No. 7,251,833 B2 and further in view of Granger et al U.S. Patent No. 6,334,189 B1.

As per **claim 11**, both Peterka et al and feig failed to explicitly disclose the method, wherein generating comprises generating each of the plurality of customer processing platform-specific keys using the identifier and a respective key generation seed value.

Granger et al discloses the method, wherein generating comprises generating each of the plurality of customer processing platform-specific keys using the identifier and a respective key generation seed value (see fig. 1).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Peterka et al and incorporate the method wherein generating comprises generating each of the plurality of customer processing platform-specific keys using the identifier and a respective key generation seed value in view of the teachings of Granger et al in order to further secure the decryption keys.

As per **claim 12**, Peterka et al and feig et al failed to explicitly disclose the method, wherein delivering to the customer processing platform a plurality of decryption keys comprises delivering the respective key generation seed values.

Granger et al discloses the method, wherein delivering to the customer processing platform a plurality of decryption keys comprises delivering the respective key generation seed values (see fig. 1; col. 10, lines 45-55).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Peterka et al and incorporate the method wherein delivering to the customer processing platform a plurality of decryption keys comprises delivering the respective key generation seed values in view of the teachings of Granger et al in order to further secure the decryption keys.

6. **Claims 14 and 43**, is rejected under 35 U.S.C. 103(a) as being unpatentable over Peterka et al U.S. Patent Application Publication No. 2002/0170053

A1 in view of Feig et al U.S. patent No. 7,251,833 B2 and further in view of Ginter et al U.S. Patent Application Publication No. 2006/0218651 A1.

As per **claim 14**, Peterka et al discloses the method, further comprising:

delivering the plurality of encrypted sections from the customer processing platform to a second customer processing platform; and

delivering the plurality of decryption keys from the data content provider to the second customer processing platform, wherein the decryption keys are delivered in a manner such that the second customer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time.

Feig et al discloses delivering the plurality of decryption keys from the data content provider to the second customer processing platform, wherein the decryption keys are delivered in a manner such that the second customer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time (see fig. 3, step 308-314; col. 2, lines 40-65, which discloses that "it is preferred that the token keys are transmitted to the client receiver by sequentially streaming each of the token keys, one at a time, enabling a one –to-one decryption and playback of the encrypted sequential data blocks"; col. 3, lines 1-5, which discloses that preferred method further includes sequentially decrypting each of the respective plurality of encrypted sequential data blocks using corresponding one of the plurality of cryptographic token keys...and for playing back each recovered sequential data")

Ginter et al discloses delivering the plurality of encrypted sections from the customer processing platform to a second customer processing platform (fig. 28).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Peterka et al and incorporate the method of delivering the plurality of encrypted sections from the customer processing platform to a second customer processing platform in view of the teachings of Ginter et al in order to encourage wider distribution of content to other participants.

As per claim 43, both Peterka et al and feig et al failed to explicitly disclose the method, wherein receiving the plurality of encrypted sections of the data content comprises receiving the plurality of encrypted sections of the data content from another customer processing platform.

Ginter et al discloses the method, wherein receiving the plurality of encrypted sections of the data content comprises receiving the plurality of encrypted sections of the data content from another customer processing platform (fig. 28).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Peterka et al and incorporate the method of delivering the plurality of encrypted sections from the customer processing platform to a second customer processing platform in view of the teachings of Ginter et al in order to encourage wider distribution of content to other participants.

7. **Claims 16-18**, are rejected under 35 U.S.C. 103(a) as being unpatentable over Feig et al U.S. Patent No. 7,251,833 in view of Giroux et al U.S. Patent Application Publication No. 2002/0078361 A1.

As per **claims 16 and 21**, Feig et al discloses a method of receiving and controlling playback of data content at a customer processing platform, comprising:

receiving over a communications medium a plurality of encrypted sections of data content, each of which has been encrypted using a respective encryption key (fig. 3; steps 302-314; col. 1, line 55-col. 2, line 10, which discloses "plurality of sequential data blocks using corresponding token key");

and for each encrypted section:

receiving a decryption key in respect of the encrypted section (col. 2, lines 40-65, which discloses that "it is preferred that the token keys are transmitted to the client receiver by sequentially streaming each of the token keys, one at a time, enabling a one-to-one decryption and playback of the encrypted sequential data blocks"; col. 3, lines 1-5, which discloses that preferred method further includes sequentially decrypting each of the respective plurality of encrypted sequential data blocks using corresponding one of the plurality of cryptographic token keys...and for playing back each recovered sequential data");

decrypting and playing back the encrypted section using the decryption key (col. 2, lines 40-65, which discloses that "it is preferred that the token keys are transmitted to the client receiver by sequentially streaming each of the token keys, one at a time,

enabling a one –to-one decryption and playback of the encrypted sequential data blocks”; col. 3, lines 1-5, which discloses that preferred method further includes sequentially decrypting each of the respective plurality of encrypted sequential data blocks using corresponding one of the plurality of cryptographic token keys...and for playing back each recovered sequential data”).

What Feig et al does not explicitly teach is

destroying the decryption key after completing playback of the encrypted section.

Giroux et al discloses a method comprising:

destroying the decryption key after completing playback of the encrypted section (0051, which discloses that "after decrypting the section, ... immediately discards/destroys the key...").

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Feig et al and incorporate the method of destroying the decryption key after completing playback of the encrypted section in view of the teachings of Giroux et al in order to ensure that content is only used for the number of times permitted.

As per **claim 17**, Feig et al failed to explicitly disclose the method, further comprising, for each encrypted section:

destroying decrypted data content at the customer processing platform after completing playback of the encrypted section.

Giroux et al discloses a method comprising destroying decrypted data content at the customer processing platform after completing playback of the encrypted section (0051, which discloses that "after decrypting the section, ... immediately discards/destroys the key...").

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Feig et al and incorporate the method of destroying decrypted data content at the customer processing platform after completing playback of the encrypted section in view of the teachings of Giroux et al in order to ensure that content is only used for the number of times permitted.

As per **claim 18**, Feig et al discloses the method, wherein the communications medium is the public Internet (col. 1, lines 40-50).

8. **Claim 19**, is rejected under 35 U.S.C. 103(a) as being unpatentable over Feig et al U.S. Patent No. 7,251,833 in view of Giroux et al U.S. Patent Application Publication No. 2002/0078361 A1 and further in view of Granger et al U.S. Patent No. 6,334,189 B1.

As per **claim 19**, both Feig et al and Giroux et al failed to explicitly disclose the method, wherein, for each encrypted section, the encryption key is the same as the decryption key.

Granger et al discloses the method, wherein, for each encrypted section, the encryption key is the same as the decryption key (col. 10, lines 45-55).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Feig et al and incorporate the method wherein, for each encrypted section, the encryption key is the same as the decryption key in view of the teachings of Granger et al in order to ensure that content is only used for the number of times permitted.

9. **Claims 22-23**, are rejected under 35 U.S.C. 103(a) as being unpatentable over Feig et al U.S. Patent No. 7,251,833 in view of Giroux et al U.S. Patent Application Publication No. 2002/0078361 A1 and further in view of Watanabe U.S. Patent No. 7,114,073 B2

As per **claim 22**, both Feig et al and Giroux et al failed to explicitly disclose the method, wherein each encryption key comprises a respective customer processing platform-specific key which is determined based on an IP address of the customer processing platform.

Watanabe discloses the method, wherein each encryption key comprises a respective customer processing platform-specific key which is determined based on an IP address of the customer processing platform (col. 5, lines 17-35, which discloses that "the encryption key generating unit 105 generates the encryption key on the basis of an IP address of a user to whom the digital content is to be transmitted").

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Feig et al and incorporate the method of destroying decrypted data content at the customer processing platform after completing playback of the encrypted section in view of the teachings of Watanabe in order to ensure that content is only used by authorized users.

As per **claim 23**, Feig et al further discloses the method, wherein receiving each decryption key comprises receiving a transmission value that is determined based on the decryption key and a hardware identifier associated with the customer processing platform, further comprising, for each encrypted section: recovering the decryption key from the transmission value (col. 2, lines 40-65).

10. **Claim 20**, is are rejected under 35 U.S.C. 103(a) as being unpatentable over Feig et al U.S. Patent No. 7,251,833 in view of Giroux et al U.S. Patent Application Publication No. 2002/0078361 A1 as applied to claim 16 above, and further in view of Ginter et al U.S. Patent Application Publication No. 2006/0218651 A1.

As per **claim 20**, both Feig et al and Giroux et al failed to explicitly disclose the method, wherein receiving the plurality of encrypted sections of the data content comprises receiving the plurality of encrypted sections of the data content from another customer processing platform.

Ginter et al discloses the method, wherein receiving the plurality of encrypted sections of the data content comprises receiving the plurality of encrypted sections of the data content from another customer processing platform (fig. 28).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of feig et al and incorporate the method of delivering the plurality of encrypted sections from the customer processing platform to a second customer processing platform in view of the teachings of Ginter et al in order to encourage wider distribution of content to other participants.

Response to Arguments

11. Applicant's arguments with respect to claims 1-23 and 34-43 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

12. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Examiner's Note: Examiner has cited particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that the applicant, in preparing the responses, fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

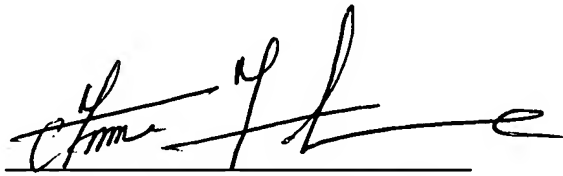
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Charles C. Agwumezie whose number is **(571) 272-6838**. The examiner can normally be reached on Monday – Friday 8:00 am – 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Fischer can be reached on **(571) 272 – 6779**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For

Art Unit: 3621

more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



Charlie Lion Agwumezie
Patent Examiner
Art Unit 3621

Acc
November 27, 2007.



ANDREW J. FISCHER
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600